Please amend the present application as follows:

Claims

The following is a copy of Applicant's claims that identifies language being added with underlining ("___") and language being deleted with strikethrough ("~~——~~"), as is applicable:

1. (Currently amended) A method for securely transmitting data between a computer and a printer, comprising:

~~converting a file for printing into a printer description language format;~~

~~encrypting said file in said printer description language format;~~

adding ~~an unencrypted~~ a header to ~~said encrypted file~~ a file that contains data to be printed;

providing an identifier in said header that ~~provides an indication of~~ identifies an encryption algorithm ~~that was used to encrypt said file~~; ~~and~~

encrypting the file with the encryption algorithm without encrypting the header; and

transmitting said encrypted file and said unencrypted header to the printer.

2. (Currently amended) The method of claim 1, further comprising receiving said encrypted file and said unencrypted header with the printer, identifying the encryption algorithm with the printer, selecting an appropriate decryption algorithm with the printer; and decrypting said encrypted file ~~by~~ with the printer using the decryption algorithm.

3. (Currently amended) The method of claim 1, ~~wherein said converting comprises~~ further comprising, prior to said encrypting, converting said file into at least one of a postscript format, a PCL format, a PDF format, and an XML format.

4. (Currently amended) The method of claim 1, further comprising: receiving said encrypted file and said unencrypted header with ~~by~~ the printer, ~~the printer~~ recognizing said identifier from said unencrypted header with the printer, validating said identifier on the printer, and selecting with the printer an appropriate decryption algorithm that is associated with the ~~computer~~ encryption algorithm.

5. (Currently amended) The method of claim 1, wherein said providing includes providing said unencrypted header ~~of said file~~ with a flag recognizable solely by the printer ~~for identifying an~~ that identifies the encryption algorithm ~~used in said encrypting~~.

6. (Canceled)

7. (Currently amended) The method of claim 5, further comprising recognizing said flag with the printer and selecting an appropriate decryption algorithm based on said recognizing.

8. (Currently amended) The method of claim 7, further comprising validating said flag on the printer by ~~entering~~ receiving a decryption key ~~into~~ with the printer that corresponds to said flag.

9. (Canceled)

10. (Previously presented) The method of claim 7, wherein selecting an appropriate decryption algorithm comprises selecting an appropriate decryption algorithm from a plurality of decryption algorithms available to the printer.

11-16. (Canceled)

17. (Currently amended) A system for securely transmitting a file in a computer network, comprising:

a first device including at least one processor for providing a file containing data to be printed with a header that ~~an encrypted file with an unencrypted header that~~ includes an identifier that ~~provides an indication as to~~ identifies an encryption algorithm, ~~that was used to encrypt the file~~ and for encrypting the file with the encryption algorithm without encrypting the file header; and

a second device including at least one processor for decrypting and outputting the file.

18. (Canceled)

19. (Currently amended) The system of claim ~~18~~ 17, wherein said at least one processor of said first device is configured to provide the file header with a flag that identifies ~~an~~ the encryption algorithm ~~that was used to encrypt the file~~.

20. (Currently amended) The system of claim 19, wherein said second device further includes an input element for ~~entry of~~ receiving a decryption key for recognition by said at least one processor of said second device and for corresponding to at least one decryption algorithm available to said at least one processor of said second device and said flag accompanying the file.

21. (Previously presented) The system of claim 17, wherein said first device comprises a computer and said second device comprises a printer, said first device having apparatus for converting the file into a printer description language format.

22. (Currently amended) The system of claim 17, wherein said ~~first~~ second device includes at least one ~~encryption algorithm that corresponds to a~~ decryption algorithm ~~available to said second device~~ that corresponds to the encryption algorithm.

23. (Previously presented) A printer, comprising:

at least one processor configured to receive an encrypted file for printing and configured to read an identifier provided in an unencrypted header associated with said encrypted file, the identifier providing an indication of an encryption algorithm that was

used to encrypt said file, said at least one processor being configured to execute a decryption algorithm associated with the encryption algorithm to decrypt said encrypted file; and

at least one printing element for printing said file.

24. (Original) The printer of claim 23, further comprising a memory connected to said at least one processor for storage of said decryption algorithm.

25-26. (Canceled)

27. (Currently amended) The printer of claim ~~26~~ 23, wherein said at least one processor selects ~~a~~ the decryption algorithm for decrypting said encrypted file from a plurality of available decryption algorithms based upon said identifier.

28. (Currently amended) The printer of claim ~~26~~ 23, further comprising an input element configured for receiving a decryption key, said decryption key corresponding to said identifier.

29. (Currently amended) The printer of claim 28, wherein said decryption key facilitates activation of ~~a~~ the decryption algorithm.